UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,137	06/30/2003	Shawn E. Wiederin	COS02007	3010

25537 7590 08/26/2008

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
08/26/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

Office Action Summary	Application No.	Applicant(s)	
	10/608,137	WIEDERIN ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10,12-16 and 19-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-10,12-16,19-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 09 May 2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below. The new ground of rejection resulted from confusion with respect to particular claim elements that arose as a result of numerous claim amendments, which resulted in the misapplication of the Rai reference. The correct application of the Rai reference is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:
/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Response to Arguments

2. Applicant argues, "SCHNEIER et al. **does not disclose a firewall system**." This argument is not persuasive because Schneier discloses on paragraph 34, with reference to figure 1, that "FIG. 1 is divided into two portions, components and systems

that operate on the customer site (***that is, within the customer's firewall***) and components and systems that operate within the SOC (that is, within the SOC firewall)."

3. Applicant's argument that "SCHNEIER et al. discloses discarding uninteresting data, and does not disclose or suggest forwarding the data for processing by a user application, as recited in claim 1", has been fully considered and is persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

KSR Int'l v. Teleflex, Inc., 127 S. Ct. 1727, 1739-40, 82 USPQ2d 1385, 1395 (2007) explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraida* [*v. AG Pro, Inc.,* 425 U.S. 273, 189 USPQ 449 (1976)] and *Anderson's-Black Rock*[*, Inc. v. Pavement Salvage Co.,* 396 U.S. 57, 163 USPQ 673 (1969)] are illustrative - a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

5. Claims 1, 4, 5, 8-10, 12-14, 16, 19, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703.

KSR Int'l v. Teleflex, Inc., 127 S. Ct. 1727, 1739-40, 82 USPQ2d 1385, 1395 (2007) explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraida* [*v. AG Pro, Inc.*, 425 U.S. 273, 189 USPQ 449 (1976)] and *Anderson's-Black Rock*[, *Inc. v. Pavement Salvage Co.*, 396 U.S. 57, 163 USPQ 673 (1969)] are illustrative - a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

6. Referring to claim 1, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of at least one interface configured to receive data transmitted via a network, a firewall configured to; receive data from the at least one interface, determine whether the data potentially contains malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data in the received data that potentially contains malicious content, intrusion detection logic configured to: receive the first data. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, and forwarding logic configured to: receive the report information, forward the report information to a remote central management system when the report information

indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of

filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 4, Schneier discloses that information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of a virtual private network gateway configured to establish a secure connection with the remote central management system.

Referring to claim 5, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using a signature-based technique.

Referring to claims 8, 9, Schneier discloses that the firewall receives filter updates from the SOC ([0037]), which meets the limitation of the firewall is configured to receive updated rule-based processing information from an external device via the network.

Referring to claim 10, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receiving data transmitted via the network, identifying first data that may contain malicious content. Interesting information collected from the firewall is sent to an anomaly engine ([0064]). The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generating report information based on the first data, forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the device. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning

that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the

Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 12, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establishing a virtual private network connection to the external device, and wherein the forwarding the report information includes forwarding the report information over the virtual private network connection.

Referring to claim 13, Schneier discloses that the SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]). Schneier does not specify that SOC determination is applied to the network traffic that corresponds to the report that was analyzed by the SOC. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6). If it is determined that the network traffic is malicious, then the network traffic is dropped (Col. 3, lines 48-54), which meets the limitation of receiving, from the external device, information indicating whether the first data is to be forwarded to the

user device, and dropping the first data when the information indicates that the first data is not to be forwarded. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious or dropped when it is determined to be malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 14, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of examining the received data for viruses using a signature-based technique.

Referring to claim 16, Schneier discloses a network monitoring system wherein a customer side firewall is configured to monitor data traffic through the network for potential unauthorized intrusions ([0035]-[0037]), which meets the limitation of receive data transmitted via a network, determine whether the data may contain malicious content using a first set of rules. The firewall receives filter updates from the SOC ([0037]), which meets the limitation of receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data. Interesting information collected from the firewall is sent to an anomaly engine ([0064]), which meets the limitation of identify first data that may contain malicious content based on the determining. The anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]), which meets the limitations of generate report information based on the first data, forward the report information to an external device when the report information indicates that the first data potentially contains malicious content. The SOC may inform the network response subsystem of the client side to block certain traffic based on the received information ([0068]), which meets the limitation of the report information allowing the remote central management system to make a forwarding decision on behalf of the processor. The anomaly engine receives only the information that cannot be identified by the negative filtering (positively identifies traffic as not being malicious) or positive filtering (positively identifies traffic as being malicious) ([0064]). The anomaly engine analyzes this received information, called "residue", and forwards only interesting information to the SOC ([0064]). Meaning

that all the "residue" that has not been provided to the SOC has been determined by the anomaly detector as being non-malicious traffic and would therefore be allowed. However, Schneier does not explicitly disclose that the network traffic corresponding to this section of the report is forwarded for processing by a user application. Joyce discloses a firewall system that performs multiple layers of filtering on network traffic to determine whether or not the network traffic is malicious (Col. 3, lines 28-58). If it is determined that the network traffic is non-malicious, then the network traffic is forwarded on through the network to its intended destination for processing (Col. 3, lines 38-43 & Col. 4, lines 1-6), which meets the limitation of forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the traffic corresponding to the report data of Schneier to be forwarded to its intended destination when it determined that the traffic is non-malicious because the purpose of filtering traffic using firewalls is to block malicious traffic while allowing legitimate traffic as taught by Joyce (Col. 1, lines 8-13). *KSR*, 127 S. Ct. at 1740, 82 USPQ2d at 1396. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another of the mere application of a known technique to a piece of prior art ready for improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known element in the fashion claimed." In this case the Joyce reference discloses the known technique of blocking/forwarding network traffic based upon a determination of the malicious or non-malicious nature of the traffic, while the

Schneier reference discloses the firewall system with which the known technique of Joyce is applicable. Additionally, one of ordinary skill in the art would have recognized that applying the technique of blocking/forwarding network traffic discussed in Joyce into the firewall system of Schneier, would have yielded predictable results.

Referring to claim 19, Schneier discloses that the anomaly engine determines what information may be worthy of additional analysis and sends the information to a resource coordinator for forwarding to a remote secure operations center (SOC) ([0064]). The information transmitted to the SOC is done so via a VPN ([0042]), which meets the limitation of establish a virtual private network tunnel with the external device and send the report information over the virtual private network tunnel.

Referring to claim 20, Schneier discloses that the firewall includes anti-virus functionality that probes for viruses using signature files ([0037]), which meets the limitation of when identifying first data that may contain malicious content, the instructions cause the processor to identify a virus using a signature-based technique.

7. Claims 6, 15, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703, and further in view of Judge, U.S. Patent No. 6,941,467. Referring to claims 6, 15, 21, Schneier does not specify that the firewall filters for spam. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to for the client-side firewall of Schneier to filter for spam because spam consumes resources that negatively impacts productivity as taught by Judge (Col. 4, lines 42-46).

8. Claims 7, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Publication No. 2002/0087882, in view of Joyce, U.S. Patent No. 6,519,703, and further in view of Bates, U.S. Patent No. 6,785,732. Referring to claims 7, 22, Schneier does not specify the type of data traffic that is received by the client-side. Bates discloses virus checking downloaded music files (Col. 10, lines 29-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made for virus-checking functionality in scan all types of data traffic, including downloaded music files, because computer viruses have emerged as a very real threat to data in today's computer systems, and checking files before they are downloaded would help to prevent virus infection as taught by Bates (Col. 1, lines 42-62).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132